



Department of Justice
Canada

National Security Litigation
& Advisory Group
PO Box 8127, Station T
Ottawa, Ontario
K1G 3H6

Ministère de la Justice
Canada

Groupe litiges et conseils
en sécurité nationale
CP 8127, Succursale T
Ottawa (Ontario)
K1G 3H6

September 9, 2016

BY HAND

Chief Justice Crampton and Mr. Justice Noël
Federal Court
90 Sparks Street
Ottawa, ON
K1A 0H9

Re: Court File No.: CSIS-GENERAL-16

Dear Chief Justice Crampton and Mr. Justice Noël:

We are writing on behalf of the Attorney General and the Canadian Security Intelligence Service further to the *En Banc* session held on June 10, 2016, to report on the status of the measures that were proposed in our letter of June 8, 2016.

As you will recall, these measures concerned both the practice before the Court in *ex parte in camera* national security matters and the review of related systems and processes governing information obtained under warrants issued under the *Canadian Security Intelligence Service Act*.

In terms of measures that pertain to the practice before the Court, as you know, the services of Mr. Murray Segal, along with those of Mr. Matthew Gourlay, a defence counsel, have been retained to provide legal and practical advice regarding the legal duties of counsel and affiants/witnesses on *ex parte* and *in camera* matters, their work to encompass the identification of best practices as well as processes. At this point, Mr. Segal and Mr. Gourlay have conducted research, completed a series of reviews and consultations with lawyers, CSIS personnel, Crown prosecutors and law enforcement officials from various jurisdictions or appearing in other type of *ex parte* matters, with private sector lawyers having acted as *amicus curiae*, and with Department of Justice lawyers having acted as independent counsel. In order to respond to concerns expressed by the Court in the meeting with messrs Segal and Gourlay, we have provided them with further background legal material including very extensive portions of the transcripts of *en banc* proceedings. Once they have upgraded their security clearance, further classified material will be provided to them.

The services of Mr. John Sims, Q.C. have also been retained to provide advice on structures and processes in the Department to achieve the standards and implement the recommendations that will be received from Mr. Segal and Mr. Gourlay.

At this point, we expect to extend the appointments of messrs Segal, Gourley (and that of Mr. Sims) to allow them to benefit from examination of further material, which will be possible upon upgrade of their clearances. As a result, their work, and that of Mr. Sims, will be completed at later dates than anticipated, likely toward the end of 2016. Their work will also serve to inform the policy that will be adopted jointly

Canada

by the Attorney General and the Service on "Fulfilling the Duty of Candour in *Ex Parte* and *In Camera* National Security Proceedings".

The review of business processes within CSIS is expected to be completed in September, as planned. The Executive Committee of the Service will receive project findings and recommendations before the end of October. In addition, the Service has embarked upon a review of its compliance governance for all operational activities.

As you will recall, during the *en banc* session held on June 10, the Director of the Service and the Deputy Attorney General both expressed their commitment towards restoring a climate of trust and respect, and in the adoption and implementation of these measures, described as important priorities for both organizations. We continue to work diligently towards that goal.

Yours truly,



Mylène Bouzigon
Senior General Counsel

cc: Michel Coulombe, Director, Canadian Security Intelligence Service
Geoff Bickert, Assistant Deputy Attorney General Litigation
Robert Frater, Chief General Counsel, Q.C.

Commissaire à la protection
de la vie privée du Canada



Privacy Commissioner
of Canada

PLS REVIEW AND
PROVIDE COMMENT.

PROTÉGÉ B AVEC PIÈCES JOINTES

22 SEP. 2016
Notre dossier : 5260-11

Monsieur Michel Coulombe
Directeur du Service canadien du renseignement de sécurité
1941, chemin Ogilvie
Ottawa (Ontario) K1J 1B7

CSIS / SCRS

SEP 26 2016

25007

DIR

Monsieur,

Vous trouverez ci-joint cinq exemplaires, en français et en anglais, du rapport de vérification final faisant état des résultats de notre examen de la façon dont la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) a été appliquée au cours des six premiers mois suivant son entrée en vigueur.

Veuillez noter que les résultats de la vérification seront publiés dans notre rapport annuel au Parlement, qui doit être déposé devant la Chambre des communes et le Sénat le 27 septembre 2016. Le rapport de vérification sera mis en ligne sur notre site Web dès cette date. Dans l'intervalle, je vous saurais gré d'en traiter le contenu en toute confidentialité.

Par ailleurs, j'aimerais vous remercier, ainsi que tous les employés du SCRS, de votre collaboration au cours de la vérification.

Si vous souhaitez discuter du contenu du rapport, n'hésitez pas à communiquer avec moi ou avec M. Steven Morgan au 819-994-6046.

Je vous prie d'agréer, Monsieur, l'expression de mes sentiments les meilleurs.

Le commissaire,

Daniel Therrien

CSIS / SCRS

25007
SEP 29 2016

p. j.

ADP / DAP

30, rue Victoria, 1^{er} étage | 30 Victoria Street, 1st Floor
Gatineau (Québec) K1A 1H3

Sans frais/Toll free 1-800-282-1376 Tél./Tel: 819-994-5444 Téléc./Fax: 819-994-5424 www.priv.gc.ca

Review of the First Six Months of the Security of Canada Information Sharing Act

1. The *Security of Canada Information Sharing Act* (SCISA) came into force on August 1, 2015. The stated purpose of the Act is to encourage and facilitate information sharing between Government of Canada institutions in order to protect against “activities that undermine the security of Canada”. In introducing the SCISA, the government stated that effective, efficient and responsible sharing of information between the various institutions of government is increasingly essential to identify, understand and respond to threats to national security. Under the Act, information may be disclosed if it is relevant to the recipient institution’s mandate or responsibilities in respect of activities that undermine the security of Canada, including in respect of the detection, identification, analysis, prevention, investigation or disruption of such activities. Protecting the security of Canadians is important, and we recognize that greater information sharing may assist in the identification and suppression of security threats.
2. The Act is broadly worded and leaves much discretion to federal entities to interpret and define “activities that undermine the security of Canada”, potentially resulting in an inconsistent approach in its application. Moreover, the scale of information sharing that could occur under this Act is unprecedented. While a preliminary review of the data suggests a limited use of SCISA during its first six months of implementation, the potential for sharing on a much larger scale combined with advances in technology allow for personal information to be analyzed algorithmically to spot trends, predict behaviour and potentially profile ordinary Canadians with a view to identifying security threats among them. Our intent in future reviews will be to examine whether law abiding citizens are indeed subject to these broad sharing powers, and if so, under what circumstances.
3. There is currently some level of review or oversight of certain federal entities responsible for national security. However, 14 of the 17 entities authorized to receive information for national security purposes under the SCISA are not subject to dedicated independent review or oversight. We note that the government has announced its intention to create a new Parliamentary Committee with responsibility for national security-related issues.
4. We initiated a review to inform stakeholders, including parliamentarians, on the extent of information sharing pursuant to the SCISA. A survey was issued to 128 Government of Canada institutions, specifically the 17 institutions which are authorized to both collect and disclose information under the SCISA and 111 federal institutions which may now disclose information to any of the 17 institutions. The survey covered the first six months that the SCISA was in force (August 1, 2015 to January 31, 2016).
5. Our survey found that during the first six months that the SCISA was in force, five institutions reported having either collected or disclosed information pursuant to the Act. [REDACTED] the Canadian Security Intelligence Service, [REDACTED] reported that collectively they received (i.e. collected), information under the SCISA on 52 occasions. The survey also revealed that collectively, [REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED] made a total of 58 disclosures under the SCISA during the same time period. All of the other 111 federal institutions surveyed reported that they had not disclosed information under the SCISA. We also made general enquiries about the nature of the sharing activities. The enquiries were made to obtain an indication of the potential risk to law abiding citizens. We asked whether information shared involved specific individuals as opposed to categories of individuals. As well, we wanted to know if the information shared included individuals not suspected of undermining the security of Canada at the time of disclosure. In responding to our survey, the entities reported that information shared under the SCISA was for named individuals suspected of undermining the security of Canada.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

9. The Treasury Board of Canada Secretariat (TBS) *Directive on Privacy Impact Assessment (PIA)* came into force in 2010. The Directive is designed to ensure privacy protection is a core consideration in the initial framing and subsequent administration of programs and activities involving personal information. This was partly in response to Canadians and parliamentarians who expressed concerns about the complex and sensitive privacy implications surrounding proactive anti-terrorism measures, the use of surveillance and privacy-intrusive technologies, the sharing of personal information across borders and the threats to privacy posed by security breaches.

[REDACTED]

11. Of the 17 entities authorized to collect information under the SCISA, 12 had undertaken some form of analysis to determine whether Privacy Impact Assessments (PIA) for their respective information sharing processes were necessary. Of these, two of the entities indicated that PIAs were deemed necessary and were under development.
12. As part of our survey, we asked institutions whether they developed policies and guidance documents to operationalize the Act. As reported above, five institutions collected and/or disclosed personal information pursuant to the SCISA during the review period. Of these, three had developed such documents. We examined them and found that they lacked specificity and detail to provide meaningful assistance to employees to help them determine whether SCISA thresholds have been met.

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Review of the First Six Months of the Security of Canada Information Sharing Act

1. The *Security of Canada Information Sharing Act* (SCISA) came into force on August 1, 2015. The stated purpose of the Act is to encourage and facilitate information sharing between Government of Canada institutions in order to protect against “activities that undermine the security of Canada”. In introducing the SCISA, the government stated that effective, efficient and responsible sharing of information between the various institutions of government is increasingly essential to identify, understand and respond to threats to national security. Under the Act, information may be disclosed if it is relevant to the recipient institution’s mandate or responsibilities in respect of activities that undermine the security of Canada, including in respect of the detection, identification, analysis, prevention, investigation or disruption of such activities. Protecting the security of Canadians is important, and we recognize that greater information sharing may assist in the identification and suppression of security threats.
2. The Act is broadly worded and leaves much discretion to federal entities to interpret and define “activities that undermine the security of Canada”, potentially resulting in an inconsistent approach in its application. Moreover, the scale of information sharing that could occur under this Act is unprecedented. While a preliminary review of the data suggests a limited use of SCISA during its first six months of implementation, the potential for sharing on a much larger scale combined with advances in technology allow for personal information to be analyzed algorithmically to spot trends, predict behaviour and potentially profile ordinary Canadians with a view to identifying security threats among them. Our intent in future reviews will be to examine whether law abiding citizens are indeed subject to these broad sharing powers, and if so, under what circumstances.
3. There is currently some level of review or oversight of certain federal entities responsible for national security. However, 14 of the 17 entities authorized to receive information for national security purposes under the SCISA are not subject to dedicated independent review or oversight. We note that the government has announced its intention to create a new Parliamentary Committee with responsibility for national security-related issues.
4. We initiated a review to inform stakeholders, including parliamentarians, on the extent of information sharing pursuant to the SCISA. A survey was issued to 128 Government of Canada institutions, specifically the 17 institutions which are authorized to both collect and disclose information under the SCISA and 111 federal institutions which may now disclose information to any of the 17 institutions. The survey covered the first six months that the SCISA was in force (August 1, 2015 to January 31, 2016).
5. Our survey found that during the first six months that the SCISA was in force, five institutions reported having either collected or disclosed information pursuant to the Act. [REDACTED] the Canadian Security Intelligence Service, [REDACTED] reported that collectively they received (i.e. collected), information under the SCISA on 52 occasions. The survey also revealed that collectively, [REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED] made a total of 58 disclosures under the SCISA during the same time period. All of the other 111 federal institutions surveyed reported that they had not disclosed information under the SCISA. We also made general enquiries about the nature of the sharing activities. The enquiries were made to obtain an indication of the potential risk to law abiding citizens. We asked whether information shared involved specific individuals as opposed to categories of individuals. As well, we wanted to know if the information shared included individuals not suspected of undermining the security of Canada at the time of disclosure. In responding to our survey, the entities reported that information shared under the SCISA was for named individuals suspected of undermining the security of Canada.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED]

9. The Treasury Board of Canada Secretariat (TBS) *Directive on Privacy Impact Assessment (PIA)* came into force in 2010. The Directive is designed to ensure privacy protection is a core consideration in the initial framing and subsequent administration of programs and activities involving personal information. This was partly in response to Canadians and parliamentarians who expressed concerns about the complex and sensitive privacy implications surrounding proactive anti-terrorism measures, the use of surveillance and privacy-intrusive technologies, the sharing of personal information across borders and the threats to privacy posed by security breaches.

[REDACTED]

11. Of the 17 entities authorized to collect information under the SCISA, 12 had undertaken some form of analysis to determine whether Privacy Impact Assessments (PIA) for their respective information sharing processes were necessary. Of these, two of the entities indicated that PIAs were deemed necessary and were under development.
12. As part of our survey, we asked institutions whether they developed policies and guidance documents to operationalize the Act. As reported above, five institutions collected and/or disclosed personal information pursuant to the SCISA during the review period. Of these, three had developed such documents. We examined them and found that they lacked specificity and detail to provide meaningful assistance to employees to help them determine whether SCISA thresholds have been met.

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED]

[REDACTED]

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Review of the First Six Months of the Security of Canada Information Sharing Act

1. The *Security of Canada Information Sharing Act* (SCISA) came into force on August 1, 2015. The stated purpose of the Act is to encourage and facilitate information sharing between Government of Canada institutions in order to protect against “activities that undermine the security of Canada”. In introducing the SCISA, the government stated that effective, efficient and responsible sharing of information between the various institutions of government is increasingly essential to identify, understand and respond to threats to national security. Under the Act, information may be disclosed if it is relevant to the recipient institution’s mandate or responsibilities in respect of activities that undermine the security of Canada, including in respect of the detection, identification, analysis, prevention, investigation or disruption of such activities. Protecting the security of Canadians is important, and we recognize that greater information sharing may assist in the identification and suppression of security threats.
2. The Act is broadly worded and leaves much discretion to federal entities to interpret and define “activities that undermine the security of Canada”, potentially resulting in an inconsistent approach in its application. Moreover, the scale of information sharing that could occur under this Act is unprecedented. While a preliminary review of the data suggests a limited use of SCISA during its first six months of implementation, the potential for sharing on a much larger scale combined with advances in technology allow for personal information to be analyzed algorithmically to spot trends, predict behaviour and potentially profile ordinary Canadians with a view to identifying security threats among them. Our intent in future reviews will be to examine whether law abiding citizens are indeed subject to these broad sharing powers, and if so, under what circumstances.
3. There is currently some level of review or oversight of certain federal entities responsible for national security. However, 14 of the 17 entities authorized to receive information for national security purposes under the SCISA are not subject to dedicated independent review or oversight. We note that the government has announced its intention to create a new Parliamentary Committee with responsibility for national security-related issues.
4. We initiated a review to inform stakeholders, including parliamentarians, on the extent of information sharing pursuant to the SCISA. A survey was issued to 128 Government of Canada institutions, specifically the 17 institutions which are authorized to both collect and disclose information under the SCISA and 111 federal institutions which may now disclose information to any of the 17 institutions. The survey covered the first six months that the SCISA was in force (August 1, 2015 to January 31, 2016).
5. Our survey found that during the first six months that the SCISA was in force, five institutions reported having either collected or disclosed information pursuant to the Act [REDACTED] the Canadian Security Intelligence Service, [REDACTED] reported that collectively they received (i.e. collected), information under the SCISA on 52 occasions. The survey also revealed that collectively, [REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED] made a total of 58 disclosures under the SCISA during the same time period. All of the other 111 federal institutions surveyed reported that they had not disclosed information under the SCISA. We also made general enquiries about the nature of the sharing activities. The enquiries were made to obtain an indication of the potential risk to law abiding citizens. We asked whether information shared involved specific individuals as opposed to categories of individuals. As well, we wanted to know if the information shared included individuals not suspected of undermining the security of Canada at the time of disclosure. In responding to our survey, the entities reported that information shared under the SCISA was for named individuals suspected of undermining the security of Canada.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

9. The Treasury Board of Canada Secretariat (TBS) *Directive on Privacy Impact Assessment (PIA)* came into force in 2010. The Directive is designed to ensure privacy protection is a core consideration in the initial framing and subsequent administration of programs and activities involving personal information. This was partly in response to Canadians and parliamentarians who expressed concerns about the complex and sensitive privacy implications surrounding proactive anti-terrorism measures, the use of surveillance and privacy-intrusive technologies, the sharing of personal information across borders and the threats to privacy posed by security breaches.

[REDACTED]

11. Of the 17 entities authorized to collect information under the SCISA, 12 had undertaken some form of analysis to determine whether Privacy Impact Assessments (PIA) for their respective information sharing processes were necessary. Of these, two of the entities indicated that PIAs were deemed necessary and were under development.
12. As part of our survey, we asked institutions whether they developed policies and guidance documents to operationalize the Act. As reported above, five institutions collected and/or disclosed personal information pursuant to the SCISA during the review period. Of these, three had developed such documents. We examined them and found that they lacked specificity and detail to provide meaningful assistance to employees to help them determine whether SCISA thresholds have been met.

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Review of the First Six Months of the Security of Canada Information Sharing Act

1. The *Security of Canada Information Sharing Act* (SCISA) came into force on August 1, 2015. The stated purpose of the Act is to encourage and facilitate information sharing between Government of Canada institutions in order to protect against “activities that undermine the security of Canada”. In introducing the SCISA, the government stated that effective, efficient and responsible sharing of information between the various institutions of government is increasingly essential to identify, understand and respond to threats to national security. Under the Act, information may be disclosed if it is relevant to the recipient institution’s mandate or responsibilities in respect of activities that undermine the security of Canada, including in respect of the detection, identification, analysis, prevention, investigation or disruption of such activities. Protecting the security of Canadians is important, and we recognize that greater information sharing may assist in the identification and suppression of security threats.
2. The Act is broadly worded and leaves much discretion to federal entities to interpret and define “activities that undermine the security of Canada”, potentially resulting in an inconsistent approach in its application. Moreover, the scale of information sharing that could occur under this Act is unprecedented. While a preliminary review of the data suggests a limited use of SCISA during its first six months of implementation, the potential for sharing on a much larger scale combined with advances in technology allow for personal information to be analyzed algorithmically to spot trends, predict behaviour and potentially profile ordinary Canadians with a view to identifying security threats among them. Our intent in future reviews will be to examine whether law abiding citizens are indeed subject to these broad-sharing powers, and if so, under what circumstances.
3. There is currently some level of review or oversight of certain federal entities responsible for national security. However, 14 of the 17 entities authorized to receive information for national security purposes under the SCISA are not subject to dedicated independent review or oversight. We note that the government has announced its intention to create a new Parliamentary Committee with responsibility for national security-related issues.
4. We initiated a review to inform stakeholders, including parliamentarians, on the extent of information sharing pursuant to the SCISA. A survey was issued to 128 Government of Canada institutions, specifically the 17 institutions which are authorized to both collect and disclose information under the SCISA and 111 federal institutions which may now disclose information to any of the 17 institutions. The survey covered the first six months that the SCISA was in force (August 1, 2015 to January 31, 2016).
5. Our survey found that during the first six months that the SCISA was in force, five institutions reported having either collected or disclosed information pursuant to the Act [REDACTED] the Canadian Security Intelligence Service, [REDACTED] reported that collectively they received (i.e. collected), information under the SCISA on 52 occasions. The survey also revealed that collectively, [REDACTED]

der the SCISA during the same time period. All of
rted that they had not disclosed information under
t the nature of the sharing activities. The enquiries
ial risk to law abiding citizens. We asked whether
as opposed to categories of individuals. As well, we
ed individuals not suspected of undermining the
esponding to our survey, the entities reported that
ed individuals suspected of undermining the

07/11/2015 S.S.

LA LOI
RÈGLEMENT

PROVA

RÉVISÉ
SUR LA
PERSONNEL

DE LA LOI
INFORMATION

9. The Treasury Board of Canada Secretariat (TBS) *Directive on Privacy Impact Assessment (PIA)* came into force in 2010. The Directive is designed to ensure privacy protection is a core consideration in the initial framing and subsequent administration of programs and activities involving personal information. This was partly in response to Canadians and parliamentarians who expressed concerns about the complex and sensitive privacy implications surrounding proactive anti-terrorism measures, the use of surveillance and privacy-intrusive technologies, the sharing of personal information across borders and the threats to privacy posed by security breaches.

[REDACTED]

11. Of the 17 entities authorized to collect information under the SCISA, 12 had undertaken some form of analysis to determine whether Privacy Impact Assessments (PIA) for their respective information sharing processes were necessary. Of these, two of the entities indicated that PIAs were deemed necessary and were under development.
12. As part of our survey, we asked Institutions whether they developed policies and guidance documents to operationalize the Act. As reported above, five institutions collected and/or disclosed personal information pursuant to the SCISA during the review period. Of these, three had developed such documents. We examined them and found that they lacked specificity and detail to provide meaningful assistance to employees to help them determine whether SCISA thresholds have been met.

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE CSIS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[illegible]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Review of the First Six Months of the Security of Canada Information Sharing Act

1. The *Security of Canada Information Sharing Act* (SCISA) came into force on August 1, 2015. The stated purpose of the Act is to encourage and facilitate information sharing between Government of Canada institutions in order to protect against "activities that undermine the security of Canada". In introducing the SCISA, the government stated that effective, efficient and responsible sharing of information between the various institutions of government is increasingly essential to identify, understand and respond to threats to national security. Under the Act, information may be disclosed if it is relevant to the recipient institution's mandate or responsibilities in respect of activities that undermine the security of Canada, including in respect of the detection, identification, analysis, prevention, investigation or disruption of such activities. Protecting the security of Canadians is important, and we recognize that greater information sharing may assist in the identification and suppression of security threats.
2. The Act is broadly worded and leaves much discretion to federal entities to interpret and define "activities that undermine the security of Canada", potentially resulting in an inconsistent approach in its application. Moreover, the scale of information sharing that could occur under this Act is unprecedented. While a preliminary review of the data suggests a limited use of SCISA during its first six months of implementation, the potential for sharing on a much larger scale combined with advances in technology allow for personal information to be analyzed algorithmically to spot trends, predict behaviour and potentially profile ordinary Canadians with a view to identifying security threats among them. Our intent in future reviews will be to examine whether law abiding citizens are indeed subject to these broad sharing powers, and if so, under what circumstances.
3. There is currently some level of review or oversight of certain federal entities responsible for national security. However, 14 of the 17 entities authorized to receive information for national security purposes under the SCISA are not subject to dedicated independent review or oversight. We note that the government has announced its intention to create a new Parliamentary Committee with responsibility for national security-related issues.
4. We initiated a review to inform stakeholders, including parliamentarians, on the extent of information sharing pursuant to the SCISA. A survey was issued to 128 Government of Canada institutions, specifically the 17 institutions which are authorized to both collect and disclose information under the SCISA and 111 federal institutions which may now disclose information to any of the 17 institutions. The survey covered the first six months that the SCISA was in force (August 1, 2015 to January 31, 2016).
5. Our survey found that during the first six months that the SCISA was in force, five institutions reported having either collected or disclosed information pursuant to the Act [REDACTED] the Canadian Security Intelligence Service, [REDACTED] [REDACTED] reported that collectively they received (i.e. collected), information under the SCISA on 52 occasions. The survey also revealed that collectively, [REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED] made a total of 58 disclosures under the SCISA during the same time period. All of the other 111 federal institutions surveyed reported that they had not disclosed information under the SCISA. We also made general enquiries about the nature of the sharing activities. The enquiries were made to obtain an indication of the potential risk to law abiding citizens. We asked whether information shared involved specific individuals as opposed to categories of individuals. As well, we wanted to know if the information shared included individuals not suspected of undermining the security of Canada at the time of disclosure. In responding to our survey, the entities reported that information shared under the SCISA was for named individuals suspected of undermining the security of Canada.

[REDACTED]

[REDACTED]

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED]

9. The Treasury Board of Canada Secretariat (TBS) *Directive on Privacy Impact Assessment (PIA)* came into force in 2010. The Directive is designed to ensure privacy protection is a core consideration in the initial framing and subsequent administration of programs and activities involving personal information. This was partly in response to Canadians and parliamentarians who expressed concerns about the complex and sensitive privacy implications surrounding proactive anti-terrorism measures, the use of surveillance and privacy-intrusive technologies, the sharing of personal information across borders and the threats to privacy posed by security breaches.

[REDACTED]

11. Of the 17 entities authorized to collect information under the SCISA, 12 had undertaken some form of analysis to determine whether Privacy Impact Assessments (PIA) for their respective information sharing processes were necessary. Of these, two of the entities indicated that PIAs were deemed necessary and were under development.
12. As part of our survey, we asked institutions whether they developed policies and guidance documents to operationalize the Act. As reported above, five institutions collected and/or disclosed personal information pursuant to the SCISA during the review period. Of these, three had developed such documents. We examined them and found that they lacked specificity and detail to provide meaningful assistance to employees to help them determine whether SCISA thresholds have been met.

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED]

[REDACTED]

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

**Examen de la façon dont la Loi sur la communication d'information
ayant trait à la sécurité du Canada a été mise en œuvre et appliquée au cours des six premiers mois**

1. La *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) est entrée en vigueur le 1^{er} août 2015. Elle a pour objet d'encourager les institutions fédérales à communiquer entre elles de l'information et de faciliter une telle communication afin de protéger le pays contre des « activités portant atteinte à la sécurité du Canada ». En déposant le projet de loi, le gouvernement a déclaré que la communication d'information efficiente, efficace et responsable entre les diverses institutions fédérales est de plus en plus essentielle pour cerner, comprendre et contrer les menaces à la sécurité nationale. En vertu de la Loi, l'information peut être communiquée si elle se rapporte au mandat ou aux attributions de l'institution destinataire à l'égard d'activités portant atteinte à la sécurité nationale, notamment en ce qui touche la détection, l'identification, l'analyse, la prévention, l'enquête ou la perturbation de ces activités ou une enquête sur celles-ci. Il est important de protéger la sécurité des Canadiens. Et nous sommes conscients qu'une communication accrue de l'information peut aider à cerner et à éliminer les menaces à la sécurité.
2. La LCISC est formulée en termes généraux et laisse beaucoup de latitude aux institutions fédérales pour interpréter et définir les « activités portant atteinte à la sécurité du Canada », ce qui pourrait entraîner un manque d'uniformité dans son application. De plus, l'ampleur éventuelle de la communication d'information en vertu de cette loi atteint des proportions sans précédent. Un examen préliminaire des données semble indiquer un recours limité à la LCISC pendant les six premiers mois de sa mise en œuvre, mais la possibilité d'une communication à une échelle beaucoup plus grande, combinée aux progrès technologiques, permettrait d'analyser les renseignements personnels au moyen d'algorithmes pour déceler des tendances et prévoir le comportement. Des Canadiens ordinaires pourraient ainsi faire l'objet d'un profilage visant à repérer parmi eux des individus menaçant la sécurité. Dans nos futurs examens, nous tenterons de déterminer si ces vastes pouvoirs de communication d'information touchent effectivement des citoyens respectueux des lois et, le cas échéant, dans quelles situations.
3. Certaines institutions fédérales responsables de la sécurité nationale font actuellement l'objet d'examen ou de surveillance dans une certaine mesure. Toutefois, 14 des 17 institutions autorisées en vertu de la LCISC à recevoir de l'information aux fins de la sécurité nationale ne font l'objet d'aucun examen indépendant ni d'aucune surveillance. Soulignons que le gouvernement a annoncé son intention de créer un comité parlementaire chargé des questions de sécurité nationale.
4. Nous avons amorcé un examen pour informer les intervenants, notamment les parlementaires, de l'ampleur de la communication d'information en vertu de LCISC. Nous avons aussi mené un sondage auprès de 128 institutions fédérales, soit les 17 institutions autorisées à recueillir et à communiquer de l'information en vertu de cette loi et les 111 institutions fédérales désormais autorisées à leur communiquer de l'information. Le sondage portait sur les six premiers mois suivant l'entrée en vigueur de la LCISC, soit du 1^{er} août 2015 au 31 janvier 2016.

le Service canadien du renseignement de sécurité ont affirmé avoir reçu (c'est-à-dire recueilli) de l'information en vertu de la Loi à 52 reprises au total.

[illegible][illegible][illegible]

- PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION
- [REDACTED]
9. La Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor (SCT), qui est entrée en vigueur en 2010, vise à s'assurer que la protection des renseignements personnels constitue un élément central de l'élaboration initiale et de l'administration subséquente des programmes et des activités nécessitant la collecte de renseignements personnels. Elle a été publiée en partie en réponse aux Canadiens et aux parlementaires qui avaient exprimé des préoccupations concernant les répercussions complexes et délicates, sur la vie privée, des mesures antiterroristes proactives, du recours à la surveillance et à des technologies portant atteinte à la vie privée, des échanges transfrontaliers de renseignements personnels et des atteintes à la sécurité menaçant le droit à la vie privée.
- [REDACTED]

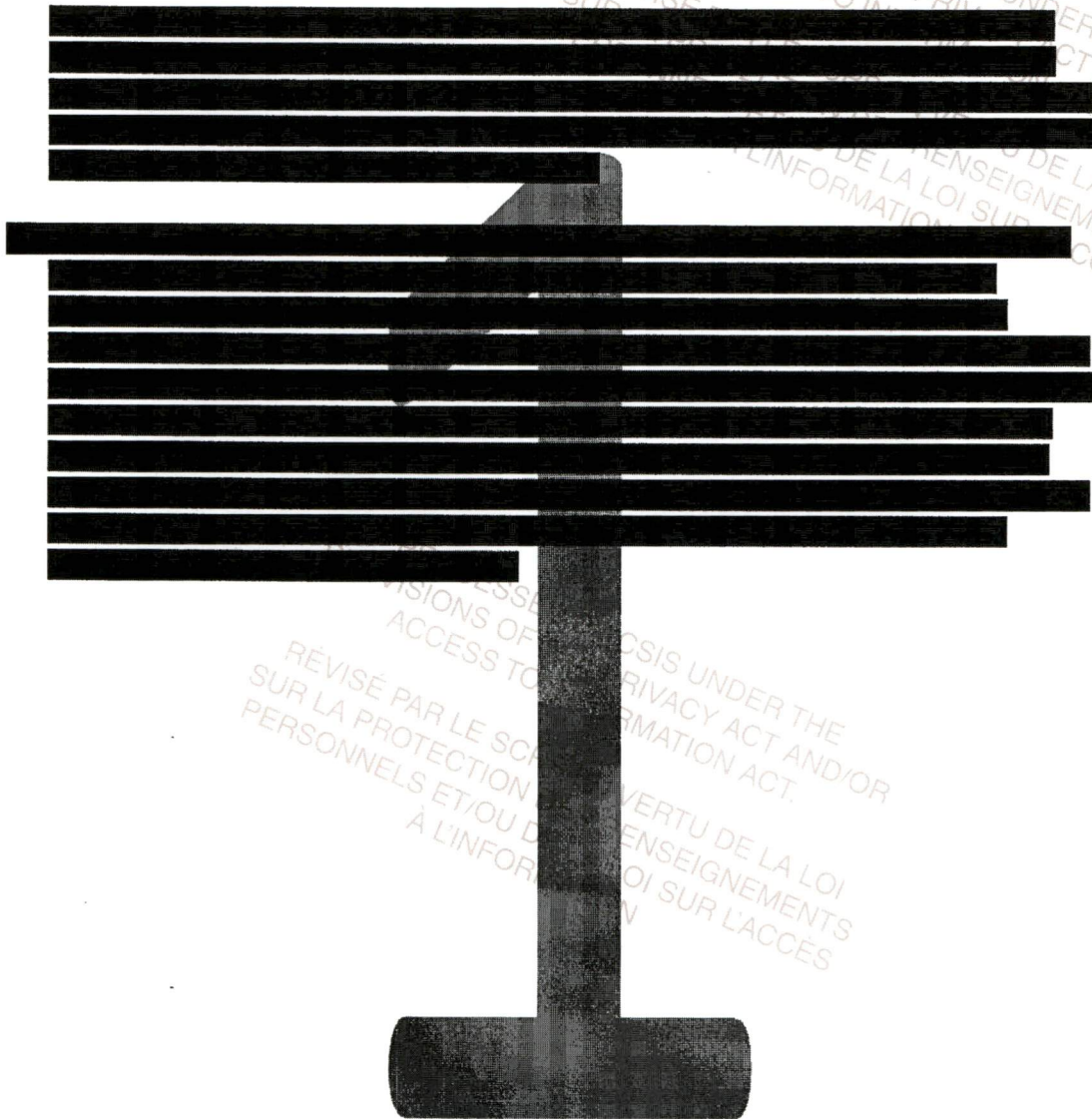
- PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION
11. Douze (12) des 17 institutions fédérales autorisées à recueillir de l'information en vertu de la LCISC ont effectué une analyse quelconque pour déterminer s'il était nécessaire d'effectuer une EFVP

relativement à leurs processus d'échange d'information. Deux d'entre elles ont estimé que cette évaluation s'imposait et elles la préparent à l'heure actuelle.

Dans le cadre de notre sondage, nous avons demandé aux institutions si elles s'étaient dotées d'une politique ou d'un document d'orientation pour donner effet à la LCISC. Comme nous l'avons déjà indiqué, cinq institutions avaient recueilli ou communiqué des renseignements personnels en vertu de cette loi au cours de la période visée par l'examen, dont trois s'étaient dotées d'une politique ou d'un document d'orientation. L'examen de ces documents nous a permis de constater qu'ils manquent de précisions et de détails pour être vraiment utiles aux employés lorsqu'il s'agit de déterminer si les seuils prévus par la LCISC ont été atteints.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION



PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

**Examen de la façon dont la Loi sur la communication d'information
ayant trait à la sécurité du Canada a été mise en œuvre et appliquée au cours des six premiers mois**

1. La *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) est entrée en vigueur le 1^{er} août 2015. Elle a pour objet d'encourager les institutions fédérales à communiquer entre elles de l'information et de faciliter une telle communication afin de protéger le pays contre des « activités portant atteinte à la sécurité du Canada ». En déposant le projet de loi, le gouvernement a déclaré que la communication d'information efficiente, efficace et responsable entre les diverses institutions fédérales est de plus en plus essentielle pour cerner, comprendre et contrer les menaces à la sécurité nationale. En vertu de la Loi, l'information peut être communiquée si elle se rapporte au mandat ou aux attributions de l'institution destinataire à l'égard d'activités portant atteinte à la sécurité nationale, notamment en ce qui touche la détection, l'identification, l'analyse, la prévention, l'enquête ou la perturbation de ces activités ou une enquête sur celles-ci. Il est important de protéger la sécurité des Canadiens. Et nous sommes conscients qu'une communication accrue de l'information peut aider à cerner et à éliminer les menaces à la sécurité.
2. La LCISC est formulée en termes généraux et laisse beaucoup de latitude aux institutions fédérales pour interpréter et définir les « activités portant atteinte à la sécurité du Canada », ce qui pourrait entraîner un manque d'uniformité dans son application. De plus, l'ampleur éventuelle de la communication d'information en vertu de cette loi atteint des proportions sans précédent. Un examen préliminaire des données semble indiquer un recours limité à la LCISC pendant les six premiers mois de sa mise en œuvre, mais la possibilité d'une communication à une échelle beaucoup plus grande, combinée aux progrès technologiques, permettrait d'analyser les renseignements personnels au moyen d'algorithmes pour déceler des tendances et prévoir le comportement. Des Canadiens ordinaires pourraient ainsi faire l'objet d'un profilage visant à repérer parmi eux des individus menaçant la sécurité. Dans nos futurs examens, nous tenterons de déterminer si ces vastes pouvoirs de communication d'information touchent effectivement des citoyens respectueux des lois et, le cas échéant, dans quelles situations.
3. Certaines institutions fédérales responsables de la sécurité nationale font actuellement l'objet d'examen ou de surveillance dans une certaine mesure. Toutefois, 14 des 17 institutions autorisées en vertu de la LCISC à recevoir de l'information aux fins de la sécurité nationale ne font l'objet d'aucun examen indépendant ni d'aucune surveillance. Soulignons que le gouvernement a annoncé son intention de créer un comité parlementaire chargé des questions de sécurité nationale.
4. Nous avons amorcé un examen pour informer les intervenants, notamment les parlementaires, de l'ampleur de la communication d'information en vertu de LCISC. Nous avons aussi mené un sondage auprès de 128 institutions fédérales, soit les 17 institutions autorisées à recueillir et à communiquer de l'information en vertu de cette loi et les 111 institutions fédérales désormais autorisées à leur communiquer de l'information. Le sondage portait sur les six premiers mois suivant l'entrée en vigueur de la LCISC, soit du 1^{er} août 2015 au 31 janvier 2016.

5. Selon le sondage, cinq institutions ont déclaré avoir recueilli ou communiqué de l'information en vertu de la LCISC au cours des six premiers mois suivant son entrée en vigueur [REDACTED]. [REDACTED] le Service canadien du renseignement de sécurité ont affirmé avoir reçu (c'est-à-dire recueilli) de l'information en vertu de la Loi à 52 reprises au total. [REDACTED] [REDACTED] ont déclaré avoir communiqué de l'information en vertu de la LCISC à 58 reprises au total au cours de cette période. Les 111 autres institutions fédérales sondées ont indiqué n'avoir communiqué aucune information en vertu de la Loi. Le sondage comportait aussi des questions d'ordre général sur la nature des activités de communication d'information. Ces questions avaient pour but d'avoir une idée du risque pour les citoyens respectueux des lois. Nous avons demandé aux institutions sondées si l'information communiquée se rapportait à des individus en particulier ou à des catégories d'individus. Nous voulions aussi savoir si cette information portait sur des personnes qui n'étaient pas soupçonnées de porter atteinte à la sécurité du Canada au moment de la communication. D'après les répondants, l'information communiquée en vertu de la LCISC se rapportait à des individus nommément désignés et soupçonnés de porter atteinte à la sécurité du Canada.

[illegible][illegible]

REVIS
LA
SON

[REDACTED]

9. La Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor (SCT), qui est entrée en vigueur en 2010, vise à s'assurer que la protection des renseignements personnels constitue un élément central de l'élaboration initiale et de l'administration subséquente des programmes et des activités nécessitant la collecte de renseignements personnels. Elle a été publiée en partie en réponse aux Canadiens et aux parlementaires qui avaient exprimé des préoccupations concernant les répercussions complexes et délicates, sur la vie privée, des mesures antiterroristes proactives, du recours à la surveillance et à des technologies portant atteinte à la vie privée, des échanges transfrontaliers de renseignements personnels et des atteintes à la sécurité menaçant le droit à la vie privée.

[REDACTED]

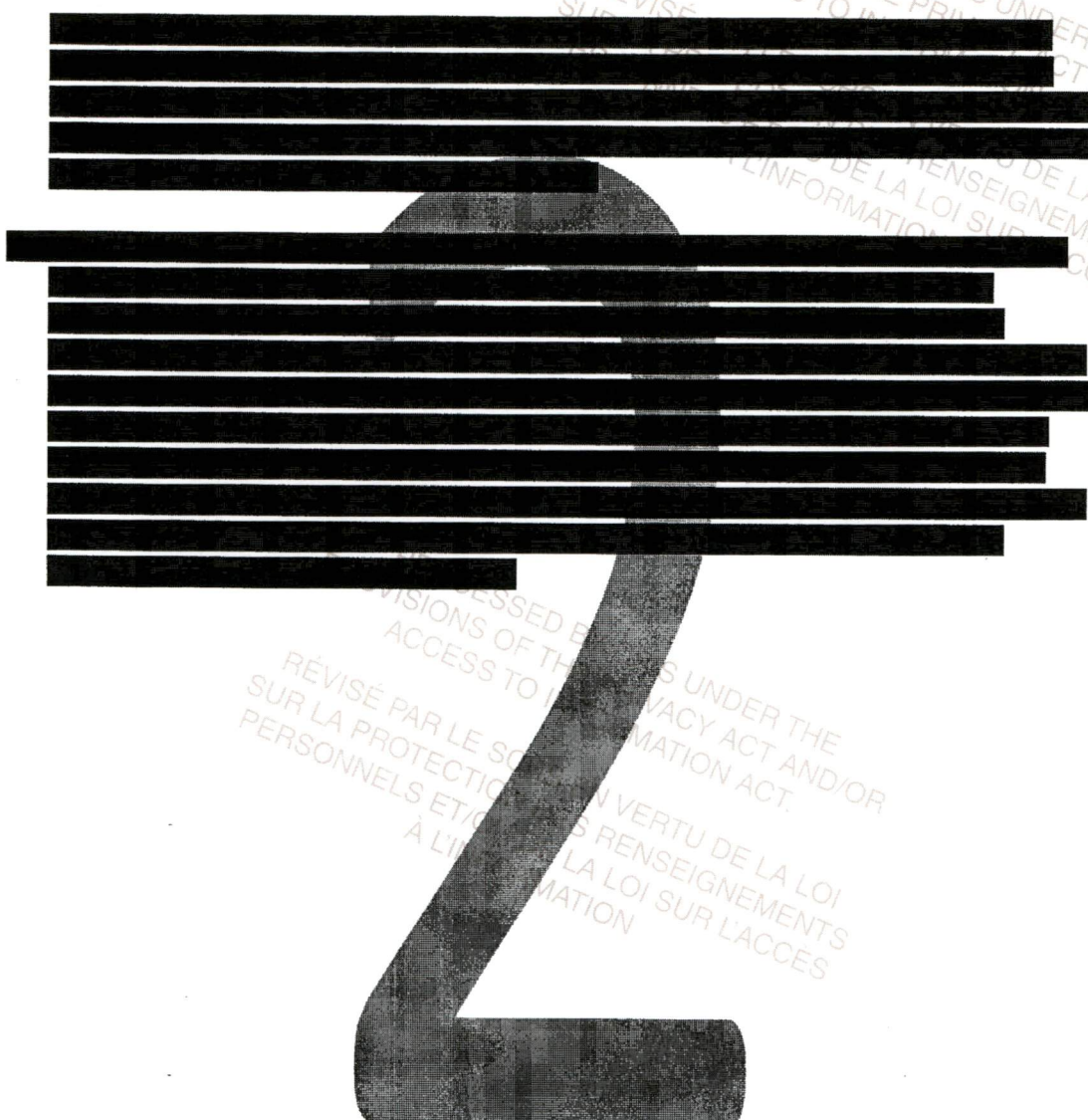
11. Douze (12) des 17 institutions fédérales autorisées à recueillir de l'information en vertu de la LCIS ont effectué une analyse quelconque pour déterminer s'il était nécessaire d'effectuer une EFVP

relativement à leurs processus d'échange d'information. Deux d'entre elles ont estimé que cette évaluation s'imposait et elles la préparent à l'heure actuelle.

■ Dans le cadre de notre sondage, nous avons demandé aux institutions si elles s'étaient dotées d'une politique ou d'un document d'orientation pour donner effet à la LCISC. Comme nous l'avons déjà indiqué, cinq institutions avaient recueilli ou communiqué des renseignements personnels en vertu de cette loi au cours de la période visée par l'examen, dont trois s'étaient dotées d'une politique ou d'un document d'orientation. L'examen de ces documents nous a permis de constater qu'ils manquent de précisions et de détails pour être vraiment utiles aux employés lorsqu'il s'agit de déterminer si les seuils prévus par la LCISC ont été atteints.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION



PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

**Examen de la façon dont la Loi sur la communication d'information
ayant trait à la sécurité du Canada a été mise en œuvre et appliquée au cours des six premiers mois**

1. La *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) est entrée en vigueur le 1^{er} août 2015. Elle a pour objet d'encourager les institutions fédérales à communiquer entre elles de l'information et de faciliter une telle communication afin de protéger le pays contre des « activités portant atteinte à la sécurité du Canada ». En déposant le projet de loi, le gouvernement a déclaré que la communication d'information efficiente, efficace et responsable entre les diverses institutions fédérales est de plus en plus essentielle pour cerner, comprendre et contrer les menaces à la sécurité nationale. En vertu de la Loi, l'information peut être communiquée si elle se rapporte au mandat ou aux attributions de l'institution destinataire à l'égard d'activités portant atteinte à la sécurité nationale, notamment en ce qui touche la détection, l'identification, l'analyse, la prévention, l'enquête ou la perturbation de ces activités ou une enquête sur celles-ci. Il est important de protéger la sécurité des Canadiens. Et nous sommes conscients qu'une communication accrue de l'information peut aider à cerner et à éliminer les menaces à la sécurité.
2. La LCISC est formulée en termes généraux et laisse beaucoup de latitude aux institutions fédérales pour interpréter et définir les « activités portant atteinte à la sécurité du Canada », ce qui pourrait entraîner un manque d'uniformité dans son application. De plus, l'ampleur éventuelle de la communication d'information en vertu de cette loi atteint des proportions sans précédent. Un examen préliminaire des données semble indiquer un recours limité à la LCISC pendant les six premiers mois de sa mise en œuvre, mais la possibilité d'une communication à une échelle beaucoup plus grande, combinée aux progrès technologiques, permettrait d'analyser les renseignements personnels au moyen d'algorithmes pour déceler des tendances et prévoir le comportement. Des Canadiens ordinaires pourraient ainsi faire l'objet d'un profilage visant à repérer parmi eux des individus menaçant la sécurité. Dans nos futurs examens, nous tenterons de déterminer si ces vastes pouvoirs de communication d'information touchent effectivement des citoyens respectueux des lois et, le cas échéant, dans quelles situations.
3. Certaines institutions fédérales responsables de la sécurité nationale font actuellement l'objet d'examen ou de surveillance dans une certaine mesure. Toutefois, 14 des 17 institutions autorisées en vertu de la LCISC à recevoir de l'information aux fins de la sécurité nationale ne font l'objet d'aucun examen indépendant ni d'aucune surveillance. Soulignons que le gouvernement a annoncé son intention de créer un comité parlementaire chargé des questions de sécurité nationale.
4. Nous avons amorcé un examen pour informer les intervenants, notamment les parlementaires, de l'ampleur de la communication d'information en vertu de LCISC. Nous avons aussi mené un sondage auprès de 128 institutions fédérales, soit les 17 institutions autorisées à recueillir et à communiquer de l'information en vertu de cette loi et les 111 institutions fédérales désormais autorisées à leur communiquer de l'information. Le sondage portait sur les six premiers mois suivant l'entrée en vigueur de la LCISC, soit du 1^{er} août 2015 au 31 janvier 2016.

(continued)

[illegible]

ont déclaré avoir communiqué de l'information en vertu de la LCISC à

[illegible][illegible]

[REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

[REDACTED]

9. La *Directive sur l'évaluation des facteurs relatifs à la vie privée* du Secrétariat du Conseil du Trésor (SCT), qui est entrée en vigueur en 2010, vise à s'assurer que la protection des renseignements personnels constitue un élément central de l'élaboration initiale et de l'administration subséquente des programmes et des activités nécessitant la collecte de renseignements personnels. Elle a été publiée en partie en réponse aux Canadiens et aux parlementaires qui avaient exprimé des préoccupations concernant les répercussions complexes et délicates, sur la vie privée, des mesures antiterroristes proactives, du recours à la surveillance et à des technologies portant atteinte à la vie privée, des échanges transfrontaliers de renseignements personnels et des atteintes à la sécurité menaçant le droit à la vie privée.

[REDACTED]

11. Douze (12) des 17 institutions fédérales autorisées à recueillir de l'information en vertu de la LCIS ont effectué une analyse quelconque pour déterminer s'il était nécessaire d'effectuer une EFVP

relativement à leurs processus d'échange d'information. Deux d'entre elles ont estimé que cette évaluation s'imposait et elles la préparent à l'heure actuelle.

■ Dans le cadre de notre sondage, nous avons demandé aux institutions si elles s'étaient dotées d'une politique ou d'un document d'orientation pour donner effet à la LCISC. Comme nous l'avons déjà indiqué, cinq institutions avaient recueilli ou communiqué des renseignements personnels en vertu de cette loi au cours de la période visée par l'examen, dont trois s'étaient dotées d'une politique ou d'un document d'orientation. L'examen de ces documents nous a permis de constater qu'ils manquent de précisions et de détails pour être vraiment utiles aux employés lorsqu'il s'agit de déterminer si les seuils prévus par la LCISC ont été atteints.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

**Examen de la façon dont la Loi sur la communication d'information
ayant trait à la sécurité du Canada a été mise en œuvre et appliquée au cours des six premiers mois**

1. La *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) est entrée en vigueur le 1^{er} août 2015. Elle a pour objet d'encourager les institutions fédérales à communiquer entre elles de l'information et de faciliter une telle communication afin de protéger le pays contre des « activités portant atteinte à la sécurité du Canada ». En déposant le projet de loi, le gouvernement a déclaré que la communication d'information efficiente, efficace et responsable entre les diverses institutions fédérales est de plus en plus essentielle pour cerner, comprendre et contrer les menaces à la sécurité nationale. En vertu de la Loi, l'information peut être communiquée si elle se rapporte au mandat ou aux attributions de l'institution destinataire à l'égard d'activités portant atteinte à la sécurité nationale, notamment en ce qui touche la détection, l'identification, l'analyse, la prévention, l'enquête ou la perturbation de ces activités ou une enquête sur celles-ci. Il est important de protéger la sécurité des Canadiens. Et nous sommes conscients qu'une communication accrue de l'information peut aider à cerner et à éliminer les menaces à la sécurité.
2. La LCISC est formulée en termes généraux et laisse beaucoup de latitude aux institutions fédérales pour interpréter et définir les « activités portant atteinte à la sécurité du Canada », ce qui pourrait entraîner un manque d'uniformité dans son application. De plus, l'ampleur éventuelle de la communication d'information en vertu de cette loi atteint des proportions sans précédent. Un examen préliminaire des données semble indiquer un recours limité à la LCISC pendant les six premiers mois de sa mise en œuvre, mais la possibilité d'une communication à une échelle beaucoup plus grande, combinée aux progrès technologiques, permettrait d'analyser les renseignements personnels au moyen d'algorithmes pour déceler des tendances et prévoir le comportement. Des Canadiens ordinaires pourraient ainsi faire l'objet d'un profilage visant à repérer parmi eux des individus menaçant la sécurité. Dans nos futurs examens, nous tenterons de déterminer si ces vastes pouvoirs de communication d'information touchent effectivement des citoyens respectueux des lois et, le cas échéant, dans quelles situations.
3. Certaines institutions fédérales responsables de la sécurité nationale font actuellement l'objet d'examen ou de surveillance dans une certaine mesure. Toutefois, 14 des 17 institutions autorisées en vertu de la LCISC à recevoir de l'information aux fins de la sécurité nationale ne font l'objet d'aucun examen indépendant ni d'aucune surveillance. Soulignons que le gouvernement a annoncé son intention de créer un comité parlementaire chargé des questions de sécurité nationale.
4. Nous avons amorcé un examen pour informer les intervenants, notamment les parlementaires, de l'ampleur de la communication d'information en vertu de LCISC. Nous avons aussi mené un sondage auprès de 128 institutions fédérales, soit les 17 institutions autorisées à recueillir et à communiquer de l'information en vertu de cette loi et les 111 institutions fédérales désormais autorisées à leur communiquer de l'information. Le sondage portait sur les six premiers mois suivant l'entrée en vigueur de la LCISC, soit du 1^{er} août 2015 au 31 janvier 2016.

5. Selon le sondage, cinq institutions ont déclaré avoir recueilli ou communiqué de l'information en vertu de la LCISC au cours des six premiers mois suivant son entrée en vigueur [REDACTED]. [REDACTED] le Service canadien du renseignement de sécurité ont affirmé avoir reçu (c'est-à-dire recueilli) de l'information en vertu de la Loi à 52 reprises au total. [REDACTED] [REDACTED] ont déclaré avoir communiqué de l'information en vertu de la LCISC à 58 reprises au total au cours de cette période. Les 111 autres institutions fédérales sondées ont indiqué n'avoir communiqué aucune information en vertu de la Loi. Le sondage comportait aussi des questions d'ordre général sur la nature des activités de communication d'information. Ces questions avaient pour but d'avoir une idée du risque pour les citoyens respectueux des lois. Nous avons demandé aux institutions sondées si l'information communiquée se rapportait à des individus en particulier ou à des catégories d'individus. Nous voulions aussi savoir si cette information portait sur des personnes qui n'étaient pas soupçonnées de porter atteinte à la sécurité du Canada au moment de la communication. D'après les répondants, l'information communiquée en vertu de la LCISC se rapportait à des individus nommément désignés et soupçonnés de porter atteinte à la sécurité du Canada.

PROCES-VERBAL
PROVISIONNEL
REVISI
SUR LA
PERSONNE
ARTU DE LA LOI
DE LA LOI SUR L'ACCÈS
A L'INFORMATION

[REDACTED]

9. La Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor (SCT), qui est entrée en vigueur en 2010, vise à s'assurer que la protection des renseignements personnels constitue un élément central de l'élaboration initiale et de l'administration subséquente des programmes et des activités nécessitant la collecte de renseignements personnels. Elle a été publiée en partie en réponse aux Canadiens et aux parlementaires qui avaient exprimé des préoccupations concernant les répercussions complexes et délicates, sur la vie privée, des mesures antiterroristes proactives, du recours à la surveillance et à des technologies portant atteinte à la vie privée, des échanges transfrontaliers de renseignements personnels et des atteintes à la sécurité menaçant le droit à la vie privée.

[REDACTED]

11. Douze (12) des 17 institutions fédérales autorisées à recueillir de l'information en vertu de la LCISC ont effectué une analyse quelconque pour déterminer s'il était nécessaire d'effectuer une EFVP

information. Deux d'entre elles ont estimé que cette mesure actuelle.

mandé aux institutions si elles s'étaient dotées d'une donner effet à la LCISC. Comme nous l'avons déjà communiqué des renseignements personnels en vertu amen, dont trois s'étaient dotées d'une politique ou documents nous a permis de constater qu'ils

[illegible]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

[REDACTED]

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION



Public Service
Labour Relations and
Employment Board

Commission des relations
de travail et de l'emploi
dans la fonction publique

Reference No. N° de référence

October 13, 2016

Mr. Michel Coulombe
Director Canadian Security Intelligence Service
DIRECTOR'S OFFICE
Station T
PO Box 9732
Ottawa, Ontario K1G 4G4

Dear Mr. Coulombe:

Re: Appointment of Full-Time & Part-Time Board Members

It has been almost two years since the Public Service Labour Relations and Employment Board carried out a consultation in accordance with section 6 of the *Public Service Labour Relations and Employment Board Act* which provides that every member, other than the Chairperson or a Vice-chairperson, must be appointed from among eligible persons whose names are on a list prepared by the Chairperson after consultation with the employers and the bargaining agents.

In order to maintain an appropriate balance in the composition of the Board as mandated by subsection 6(3) of the Act, I am seeking your participation in the process of establishing this list by requesting you to submit for consideration the names of any eligible and qualified persons whom you recommend for appointment as full-time or part-time PSLREB Board Members.

We wish to advise that, insofar as eligibility is concerned, reference should be made to section 5 of the *PSLREBA*, which stipulates that, to be eligible to hold office as a member, a person must be a Canadian citizen or a permanent resident as defined in subsection 2(1) of the *Immigration and Refugee Protection Act*; not hold any other office or employment under the employer; not be a member or hold an office or employment under an employee organization that is a bargaining agent; and, not accept or hold any other office or employment or carry on any activity that is inconsistent with the person's duties or functions.

We also wish to advise that, in considering the eligibility requirements for a PSLREB Member, whether full-time or part-time, it should be kept in mind that while involved in the full range of the Board's activities, a Member's duties will primarily be performed in the area of adjudication of Board matters, grievances, staffing complaints, and human rights complaints, as well as alternate dispute resolution processes. This will involve extensive travelling to different locations across Canada.

Canada

PO Box 1525 Station B / C.P. 1525 Succursale B, Ottawa ON K1P 0X2

-2-

Full-time Board members are appointed by the GIC on the recommendation of the Minister for a term not exceeding five years. On appointment, a full-time Member is required to reside in the National Capital Region.

Part-time members are appointed by the GIC on the recommendation of the Minister for a term not exceeding three years.

It is important that you confirm in advance with each person whose name you may be submitting that they meet the eligibility requirements set out in the *PSLREBA* and that they would be willing to accept an appointment, if selected. In addition, an up-to-date curriculum vitae should be provided for each person whose name is put forward, together with any supporting information you feel is relevant.

Attached, is the French version of this letter. Also, for ease of reference, we include a document setting out certain relevant sections of the *PSLREBA* regarding the appointment of members.

In order to avoid undue delay in the appointment process, I would ask that you provide me with the names of the persons you wish to recommend for appointment to the no later than **November 24, 2016**. Please indicate whether the person wishes to be considered for a full-time, part-time or both full-time and part-time positions. Finally, please provide all required documentation as described above.

I thank you for your cooperation in this consultation exercise. Should you have any questions or concerns regarding the above, please do not hesitate to contact the undersigned.

Sincerely yours,



Catherine Ebbs
Chairperson

Att.



Office of the Auditor General of Canada
Bureau du vérificateur général du Canada

CSIS / SCRS

AUG 03 2016

Internal audit
Vérification interne

26 July 2016

Mr. Michel Coulombe
Director
Canadian Security Intelligence Service
PO Box 9732, Station T
Ottawa, Ontario K1G 4G4

Dear Mr. Coulombe:

We wish to inform you that we are beginning a performance audit of Refugee Protection Programs to be reported in the Fall 2017 Report of the Auditor General.

As principal responsible for this performance audit, I will be contacting your Office shortly to arrange a meeting with you and/or your senior officials. At this meeting, we would like to discuss the upcoming work, including the initial scope and objective, roles and responsibilities, and information needs of the audit team.

During the audit, we may request access to, among other things, documents that may be subject to solicitor-client and other privileges. When we request access to any such documents, we do so pursuant to our powers under the *Auditor General Act*. Consequently, the disclosure of said documents by your agency is in compliance with the statutory requirements contained in the *Auditor General Act* and would not amount to waiver of any privilege attached to the documents. In addition, all documents disclosed to the Office of the Auditor General (OAG) for these purposes will be treated in strict confidence, and all present administrative arrangements with respect to the use of such documents will continue.

We would like to take this opportunity to remind you that any controlled documents we send to your agency during this audit are classified as *Protected*. As you are aware, your agency is responsible for ensuring the confidentiality of Office of the Auditor General protected documents entrusted to your care; these shall not be copied or reproduced either in whole or in part without the prior written consent of the Office of the Auditor General of Canada. You are also responsible for returning any non-electronic controlled documents to the Office one week after tabling, at the latest.

We also remind you that deputy heads are responsible for ensuring that OAG auditors have timely access to information and personnel. In accordance with sections 61 to 65 of the CSAE 3001, at the Principal's audit draft report stage, deputy heads will be asked to provide written representations related to the information provided to us.

Deputy heads are also responsible for providing guidance to their officials with respect to their roles and responsibilities during the audit process, including guidance on providing Cabinet confidence information to the OAG. Please refer to the 2010 Protocol Agreement on Access by

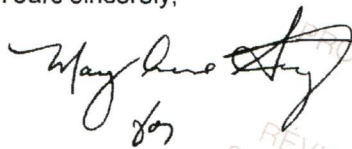
CCM 1A16-00018

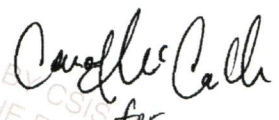
the Office of the Auditor General to Cabinet Documents between our Office and the Privy Council Office, which includes the *Guidance to Deputy Heads* issued by the Secretary of the Treasury Board. A copy of the Protocol Agreement and Guidance is attached. We ask that you forward copies of the Protocol Agreement and Guidance, with your endorsement, to your senior officials responsible for the program under audit and to your senior OAG Liaison Officer.

We would appreciate receiving by **12 August 2016** your response confirming your understanding that disclosure of any legal opinions to the OAG does not result in the loss of solicitor-client privilege, and acknowledging your responsibilities with respect to the confidentiality of OAG Canada protected documents. A suggested draft response letter is attached for your convenience. In your reply, please indicate the name and title of the senior contact person who will represent your agency in discussions during the audit. Mary Anne Strong will be the main contact person for this performance audit at the OAG.

Should you have any questions, please contact at 613-995-3708.

Yours sincerely,


Nicholas Swales
Principal (responsible for audit)


Frank Barrett
Principal (responsible for CSIS)

Encl. (2) Draft response letter
2010 Protocol Agreement on Access by the Office of the Auditor General to Cabinet Documents

cc: Chief Audit Executive, CSIS
Anne-Marie Smith, Senior General Counsel, Legal Services Branch, OAG
Nancy Y. Cheng, Assistant Auditor General, OAG

2010 Protocol Agreement on Access by the Office of the Auditor
General to Cabinet Documents

BETWEEN:

The Office of the Auditor General of Canada (OAG)

-and-

The Privy Council Office (PCO)

-and-

Treasury Board Secretariat (TBS)

WHEREAS:

Staff of the Office of the Auditor General, in order to fulfill the Auditor General's audit responsibilities, has a right of access under federal legislation to information, documents, and individuals in departments and entities which are subject to audit by the Auditor General of Canada.

The Clerk of the Privy Council is the custodian of the Cabinet confidences of all Prime Ministers.

The Auditor General's access to certain Cabinet confidences is set out in Orders-in-Council which were approved in 1985 and 2006.

In May 2010, guidance was issued to Deputy Heads on providing the Office of the Auditor General access to information in certain Cabinet Confidences.

The parties wish to establish a process whereby any dispute about OAG access to information may be resolved expeditiously in a spirit of professional cooperation.

NOW THEREFORE, THE PARTIES AGREE AS FOLLOWS:

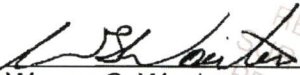
1. The Auditor General has access to certain Cabinet Confidences information as set out in Orders in Council, P.C. 1985-3783 of 27 December 1985, and P.C. 2006-1289 of November 6, 2006, copies of which are attached to this Agreement.
2. Auditors may encounter a situation where an entity restricts OAG access to any document or information on the basis that it is a Cabinet Confidence to which the OAG does not have a right of access. Where the auditors and the departmental or entity officials have been unable to resolve the access matter in dispute, they will use the measures set out in this Protocol to resolve the access matter. They may wish to consult their respective Legal Services or other officials for guidance.
3. As noted in the attached Guidance document, departmental or entity officials should be able to provide Cabinet Confidence information to the OAG within 20 working days of the OAG original request or inform the OAG of a denial of access. If the access dispute has not been resolved to the satisfaction of the OAG the Assistant Auditor General responsible for the audit will so inform the responsible Deputy Head within five working days of the denial. The Deputy Head and the Assistant Auditor General may agree to an extension of these periods.
4. The Deputy Head, with a view to resolution of the matter may consult, if necessary, with departmental or entity officials and the Assistant Auditor General responsible for the audit. The responsible Deputy Head will rely on the attached Guidance in coming to a decision.
5. The Deputy Head will inform the Assistant Auditor General of his or her decision within 10 working days of being informed of the dispute by the Assistant Auditor General. Any extensions of this deadline must be agreed upon by the Assistant Auditor General to ensure that delays in receiving the requested information will not compromise the Auditor General's ability to perform his or her statutory responsibilities.
6. If the Auditor General is of the view that his or her officials are being improperly denied access to Cabinet Confidences in the department by the Deputy Head, the Auditor General will refer the matter to the Clerk of the Privy Council, who will consider any representations from the OAG and departmental or entity officials that he or she considers necessary in order to resolve the matter. When the Clerk of the Privy Council concludes that the

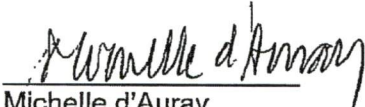
information is appropriately characterized as a Cabinet Confidence which should not be disclosed to the OAG, he or she will provide reasons for the decision in writing to the Auditor General.

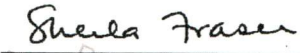
- 7: The parties will participate in periodic meetings annually or more frequently on the request of one or more parties, to review the extent to which this Protocol Agreement is achieving its intended result of resolution of issues of access to information by the OAG and to ensure, in a spirit of professional cooperation, that access to information by the OAG is provided as expeditiously as possible.

This Agreement made this 12th day of May, 2010.

For:


Wayne G. Wouters
Privy Council Office


Michelle d'Auray
Treasury Board Secretariat


Sheila Fraser
Office of the Auditor General

Guidance to Deputy Heads, departmental and entity legal counsel and OAG audit liaisons on providing the Auditor General access to information in certain confidences of the Queen's Privy Council (Cabinet Confidences)

- 1 The purpose of providing access to information and documents is to enable the Auditor General of Canada to fulfil his or her statutory responsibilities. This includes assessing, in performance and financial audits, the public accounts and special examinations, whether there has been due regard to economy, efficiency and environmental effects of government spending, and whether compliance with financial, management and other authorities has been addressed. The Auditor General and her staff (OAG) assess whether officials have in effect performed their "due diligence"; they do not, however, assess government policies and Cabinet decisions.
- 2 The Auditor General Act (s. 13) provides the OAG with broad access to information and documents the Auditor General considers necessary to carry out audits and examinations, and to personnel for the purpose of interviews and explanations. The mere fact that documents would not be released under the *Access to Information Act* does not constitute a limitation to the right of the OAG auditors to have access to them. OAG access to Cabinet Confidences is addressed through this Guidance. Unless strictly excluded by this Guidance or by the Orders in Council referred to in paragraph 4, departments and entities will provide to the OAG the information requested.
- 3 Deputy Heads are responsible for ensuring that OAG auditors have timely access to information and personnel to carry out their audits and examinations. Officials should be able to provide Cabinet Confidence information to the OAG within 20 working days of the request, or notify the OAG of any difficulties in doing so. All departmental and entity officials are required to follow this Guidance in providing Cabinet Confidences and other information and documents to the OAG. Deputy Heads are responsible for providing guidance to their officials with respect to their roles and responsibilities during the audit process, including guidance in providing Cabinet Confidence information to the OAG.
- 4 The OAG's access to records presented to Council¹, including Memoranda to Cabinet and Decks, Records of Cabinet Decisions, and Treasury Board Submissions, Treasury Board Aides-mémoire and Decisions, is set out in Orders in Council approved in December 1985 and in November 2006 (attached for reference). Cabinet Confidences created prior to February 2006 are governed by the December 1985 Order in Council. The Privy Council Office provides access to records presented to Council and final decisions of Council; the Treasury Board Secretariat provides access to Submissions and Aides-mémoire to the Treasury Board and decisions of the Treasury Board.
- 5 The OAG is entitled to explanations, analyses of problems or policy options contained in a record presented to Council (including annexes and appendices to such records where they deal with such explanations, analyses of problems and policy options) and its final decisions, but not information revealing views, opinions, advice or recommendations to Council. Where the decision on the policy options refers to approval of an annex or other record, sufficient information as to the contents of the annex or record will be provided to the OAG to inform the Auditor General of the substance of the decision.

¹ For the purposes of this Guidance, "Council" means the Queen's Privy Council for Canada, committees of the Queen's Privy Council for Canada, Cabinet and committees of Cabinet, which includes the Treasury Board.

- 6 The OAG is entitled to explanations, analyses of problems or policy options contained in or prepared by departmental, entity or Treasury Board Secretariat officials in relation to a Treasury Board Submission or Treasury Board Aide-mémoire, but not information revealing views, opinions, advice or recommendations presented to a Treasury Board Minister or to the Treasury Board, such as set out in a Précis. The following are examples of the types of information to be provided:
- a) All information exchanged (through email or other documented means) that represent comments, questions and responses on draft and final Treasury Board submissions;
 - b) Any evidence regarding compliance with Treasury Board policies, guidelines and/or authorities delegated by Treasury Board; and
 - c) Departmental, entity or Treasury Board Secretariat analysis supporting a Treasury Board Submission or Treasury Board Aide-mémoire or draft Treasury Board Submission or draft Treasury Board Aide-mémoire.
- 7 For greater certainty, it is understood that the agenda and deliberations, communications and discussions between and among Ministers on matters relating to the making of government decisions and formulation of government policy, and draft legislation, constitute Cabinet Confidences that continue to be exempted from disclosure to the OAG.
- 8 Where officials are in doubt about providing information to the OAG, because it may constitute a Cabinet Confidence to which the OAG is not entitled, they should consult their Legal Services and/or the Privy Council Office for guidance in the characterization of the documents prior to releasing or refusing to release the information to the OAG.
- 9 OAG auditors and departmental or entity officials will work diligently to resolve any access to information matter in dispute. Disputes as to the characterization of information or documents or access by the OAG to particular documents will be addressed using the 2010 Protocol Agreement (attached for reference).

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION



CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

P. C. 2006-1289
November 6, 2006

Her Excellency the Governor General in Council, on the recommendation of the Prime Minister, hereby directs that the Auditor General of Canada be granted access to the following information contained in a confidence of the Queen's Privy Council for Canada, as defined in subsection 39(2) of the *Canada Evidence Act*, that comes into existence on or after February 6, 2006, and that relates to public expenditures:

- (a) a submission to the Governor in Council,
- (b) a submission as presented to the Treasury Board and any explanations, analyses of problems or policy options contained in or prepared by officials in relation to the submission, but not information revealing views, opinions, advice or recommendations presented to a Treasury Board Minister or to the Treasury Board,
- (c) any explanations, analyses of problems or policy options contained in a record presented to Council, as defined in subsection 39(3) of the *Canada Evidence Act* ("Council"), for consideration by Council in making decisions but not information revealing a recommendation or proposal presented to Council by a Minister of the Crown,
- (d) a final decision of Council, and
- (e) a decision of the Treasury Board,

all of which information remains a confidence of the Queen's Council for Canada for the purposes of any Act of Parliament.

CERTIFIED TO BE A TRUE COPY-COPIÉ CERTIFIÉ CONFORMÉ

CLERK OF THE PRIVY COUNCIL-LE GREFFIER DU CONSEIL PRIVÉ



PRIVY COUNCIL • CONSEIL PRIVÉ

HER EXCELLENCY THE GOVERNOR GENERAL IN COUNCIL, upon the recommendation of the Prime Minister, hereby directs that the Auditor General of Canada be granted access to the following information contained in a confidence of Council (as defined under subsection 36.3(3) of the Canada Evidence Act) that comes into existence on or after January 1, 1986, and that relates to public expenditures,

- (a) a Submission to the Governor in Council;
- (b) a Submission to the Treasury Board;
- (c) any explanations, analyses of problems or policy options contained in a Memorandum or Discussion Paper presented to Council for consideration by Council in making decisions but not information revealing a recommendation or proposal presented to Council by a Minister of the Crown;
- (d) a final decision of Council; and
- (e) a decision of Treasury Board.

CERTIFIED TO BE A TRUE COPY - COPIE CERTIFIÉE CONFOR

CLERK OF THE PRIVY COUNCIL - LE GREFFIER DU CONSEIL PR

Canadian Security
Intelligence Service



Director - Directeur

Service canadien du
renseignement de sécurité

SECRET

SEP 21 2016

Dear

I have recently been advised of your departure as
Your efforts in support of the relationship between and the
Canadian Security Intelligence Service (CSIS) during your tenure have been very much
appreciated.

Our organizations have had a positive liaison partnership over the past several
years. I assure you that CSIS remains committed to enhancing our level of engagement with your
successor, and identifying areas for further collaboration
on security issues of mutual interest.

It was a pleasure to meet with you during the
and I wish you success in your future endeavours.

Sincerely,

Michel Coulombe

Canadian Security
Intelligence Service



Director - Directeur

Service canadien du
renseignement de sécurité

SECRET

SEP 21 2016

Dear

I have recently been advised of your appointment as
On behalf of the Canadian Security Intelligence Service (CSIS), I
would like to offer my sincere congratulations.

CSIS and have built a positive liaison relationship over the years and we look forward to continuing the development of such collective efforts under your leadership. I wish to assure you that CSIS remains committed to further developing this partnership, and exploring opportunities to enhance cooperation on security issues of mutual interest.

Once again, please accept my congratulations on your appointment. I wish you every success in your new position.

Sincerely,

Michel Coulombe

Canadian Security
Intelligence Service



Director - Directeur

Service canadien du
renseignement de sécurité

SECRET

SEP 24 2016

Dear :

Thank you for your recent letter informing me of your appointment as On behalf of the Canadian Security Intelligence Service (CSIS), I would like to offer my sincere congratulations.

CSIS and I have built a positive liaison relationship over the years and we look forward to continuing the development of such collective efforts under your leadership. I wish to assure you that CSIS remains committed to further developing this partnership, and exploring opportunities to enhance cooperation on security issues of mutual interest.

Once again, please accept my congratulations on your appointment. I wish you every success in your new position.

Sincerely,

Michel Coulombe

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

P. O. Box 9732, Station "T", Ottawa, Ontario K1G 4G4

C. P. 9732, Succursale "T", Ottawa (Ontario) K1G 4G4

Canadian Security
Intelligence Service



Director - Directeur

Service canadien du
renseignement de sécurité

SECRET

SEP 22 2016

Dear

Thank you for your recent letter expressing appreciation for the Canadian Security Intelligence Service's (CSIS) assistance to the

Our organizations have had a positive partnership over the past several years, and CSIS appreciated the opportunity to assist in ensuring a successful security environment. We remain committed to continuing this positive level of cooperation, and enhancing our level of engagement on security issues of mutual interest.

I have also received your separate request for to continue to use CSIS information on foreign fighters. as part of the efforts to enhance its security measures for Please rest assured that CSIS fully supports this request and has advised your liaison office in Ottawa in this regard.

It was a pleasure to meet with you during the and I wish you and your organization every success in security preparations for

Sincerely,

Michel Coulombe

P.O. Box 9732, Station "T", Ottawa, Ontario K1G 4G1

C. P. 9732, Succursale "T", Ottawa (Ontario) K1G 4G4

Canadian Security
Intelligence Service



Director - Directeur

Service canadien du
renseignement de sécurité

SECRET

OCT - 6 2016

Dear

I have recently been advised of your departure as
Your efforts in support of the relationship that exists between the
and the Canadian Security Intelligence Service (CSIS) have been very much appreciated.

Our organizations have had a positive liaison relationship over the years, and I
assure you that CSIS remains committed to further developing this partnership and identifying
potential areas of future cooperation on security issues of mutual interest.

Thank you for your support during your tenure as
you every success in your future endeavours.

and I wish

Sincerely,

Michel Coulombe

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

P. O. Box 9732, Station "T", Ottawa, Ontario K1G 4G4

C. P. 9732, Succursale "T", Ottawa (Ontario) K1G 4G4

Canadian Security
Intelligence Service



Director - Directeur

Service canadien du
renseignement de sécurité

SECRET

OCT - 4 2016

Dear

I have recently been advised of your departure as
Your efforts in support of the relationship that exists
between the and the Canadian Security Intelligence Service (CSIS) have been very much
appreciated.

Our organizations have had a positive liaison relationship over the years and I
assure you that CSIS remains committed to further developing this partnership with your
successor,

Thank you for your support during your tenure as
and I wish you every success in your future endeavours.

Sincerely,

Michel Coulombe

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

P.O. Box 9732, Station "T", Ottawa, Ontario K1G 4G4

C. P. 9732, Succursale "T", Ottawa (Ontario) K1G 4G4

Canadian Security
Intelligence Service



Director - Directeur

Service canadien du
renseignement de sécurité

SECRET

OCT - 4 2016

Dear]

I have recently been informed of your appointment as
On behalf of the Canadian Security Intelligence Service
(CSIS), I wish to offer my sincere congratulations.

CSIS and the have built a positive liaison relationship over the years, and we
look forward to identifying potential areas of future cooperation on security issues of mutual
interest.

I would like to again express my congratulations on your appointment, and I wish
you the best in your new position.

Sincerely,

Michel Coulombe

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

P. O. Box 9732, Station "T", Ottawa, Ontario K1G 4G4

C. P. 9732, Succursale "T", Ottawa (Ontario) K1G 4G4

Canadian Security
Intelligence Service



Director - Directeur

Service canadien du
renseignement de sécurité

SECRET

SEP 24 2016

Dear

Thank you for your recent letter advising me of your retirement as
relationship between and the Canadian Security Intelligence Service (CSIS) during your
tenure have been very much appreciated. Your efforts in support of the

Our organizations have had a positive liaison partnership over the past several
years. I assure you that CSIS remains committed to enhancing our level of engagement with your
successor, and to identifying areas for further collaboration on
security issues of mutual interest.

On behalf of our Service, I wish to thank you for your valued cooperation and
wish you every success in your future endeavours.

Sincerely,


Michel Coulombe

Canadian Security
Intelligence Service



Director - Directeur

Service canadien du
renseignement de sécurité

SECRET

NOV - 3 2016

Mr. Daniel Therrien
Privacy Commissioner
30 Victoria Street
Gatineau, Quebec
K1A 1H3

Dear Mr. Therrien:

This letter is to inform you of the Federal Court's decision of October 4, 2016 regarding, amongst other things, the Canadian Security Intelligence Service's (CSIS) duty of candour and retention of associated data linked with third party communications collected pursuant to section 21 of the *CSIS Act*. We are advising you of this matter in the interest of full transparency. As we work to address the Court's findings, we are committed to cooperate fully with the Office of the Privacy Commissioner (OPC) to determine the privacy impacts of the decision, should it be interested in the issue.

In 2006, CSIS' Operational Data Analysis Centre (ODAC) was established to derive more value from associated data. The exploitation of such data by ODAC enables the Service to effectively analyze threats to the security of Canada over time.

ODAC's activities are invaluable in relation to the exercise of CSIS' mandate.

In December 2015, in the context of an application to renew and obtain new warrants for targeted individuals, CSIS proposed amendments to certain warrant conditions. Owing to a finding in the 2014-2015 Annual Report tabled by the Minister on behalf of the Security Intelligence Review Committee, the Court requested that the collection, use, retention and destruction of associated data (referred to by SIRC as metadata) collected under warrants also be addressed.

For reference, metadata and associated data both refer to information around a communication; neither reveals the purpose of the communication nor any part of its content. Within CSIS, metadata and associated data, the latter being the term used in our warrant applications, applies specifically to communications collected under warrant. That said, the Federal Court decision focuses on third party communications and found the Service's retention

of third party associated data deemed to be unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs is illegal.

Given this decision, the Service is actively reviewing related policies, processes and systems. In the interim, however, CSIS immediately restricted access and halted use and analysis of associated data. As a matter of operational priority, efforts are currently underway to identify and restore access to threat-related data.

The decision does not make findings regarding the privacy expectations of individuals, nor does it weigh the state's interests against private interests as it relates to the use of such data for investigative purposes. CSIS did, however, make submissions to the Court in this regard. As you will know, CSIS completed a Privacy Impact Assessment (PIA) on the Operational Data Analysis Centre, submitted to your office in 2010. In subsequent correspondence, CSIS undertook to update the PIA as ODAC evolved and your office recommended the same. Further to the Federal Court decision, a review of the PIA is currently under way.

Clearly, we welcome the opportunity to work with your office on this update, as well as to answer any questions you may have related to recent developments. We take very seriously the need to consider and account for potential privacy impacts in our activities. I also wish to emphasize that the Service recognizes the importance of maintaining a productive and collaborative relationship with your office.

Should you wish to discuss this issue further, I would be pleased to speak with you in person.

Sincerely,



Michel Coulombe

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

August 12, 2016

Director
Canadian Security Intelligence Service
P.O. Box 9732
Postal Station "T"
Ottawa, Ontario
K1G 4G4

CSIS / SCRS

24741

AUG 22 2016

ADP / DAP

Xref: 09-03958

CSIS / SCRS

AUG 16 2016

SUBJECT : Complaint about CSIS Activities under Section 41 of the CSIS Act

DIR

CSIS / SCRS

Dear Sir/Madam,

AUG 18 2016

DAP

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

kind regards,

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Canadian Security Intelligence Service
CSIS Director
P.O. Box 9732
Postal Station "T"
Ottawa, Ontario
K1G 4G4

CSIS/SCRS

24990

SEP 22 2018

ADP/DAP

Sept 13, 2016

Xref: 22/60, 21014

Dear Mr. Coulombe:

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Please accept this letter as a notification
that one of the persons that you have
as a CSIS Informant, is known to
me.

I have discovered that you have a
woman who is a CSIS Informant, or
another ^{classification} CSIS person you have as part
of your federal entity.

Please be advised of this information.
Regards,

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.

September 12, 2016

CSIS / SCRS

SEP 21 2016

DIR

Director Michel Coulombe
Canadian Security Intelligence Service
P.O. Box 9732, Station T
Ottawa ON K1G 4G4

CSIS / SCRS

SEP 23 2016

24995

ADP / DAP

Dear Director:

I would like to offer my services as a Contract Intelligence Analyst for the Canadian
Security Intelligence Service.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

sincerely,

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION